2022-2028年中国网络公共安全市场深度分析与市场调查预测报告

报告目录及图表目录

北京迪索共研咨询有限公司
www.cction.com

一、报告报价

《2022-2028年中国网络公共安全市场深度分析与市场调查预测报告》信息及时，资料详实，指导性强，具有独家，独到，独特的优势。旨在帮助客户掌握区域经济趋势，获得优质客户信息，准确、全面、迅速了解目前行业发展动向，从而提升工作效率和效果，是把握企业战略发展定位不可或缺的重要决策依据。

官方网站浏览地址：http://www.cction.com/report/202112/259838.html

报告价格：纸介版8000元 电子版8000元 纸介+电子8500元

北京迪索共研咨询有限公司
订购电话: 400-700-9228(免长话费) 010-69365838
海外报告销售: 010-69365838
Email: kefu@gonyn.com
联系人：李经理

特别说明：本PDF目录为计算机程序生成，格式美观性可能有欠缺；实际报告排版规则、美观。

二、说明、目录、图表目录

网络安全服务种类众多，人、数据、工具、流程形成完整解决方案，目前安全服务人才缺口较大　目前网络安全服务主要分为六大类即：咨询规划、安全运营服务、专业技术服务、安全演练、安全数据分析以及考试与培训。目前网络安全服务主要分类　1 咨询规划从满足合规到“关口前移”，让安全成为真正的信息系统内生安全：咨询规划是安全服务最基本内容，过去大部分安全厂商等级保护咨询服务遵循国家等级保护各级要求，帮助客户进行信息系统达标建设，确保用户严格按照等级保护的过程规划并建设自己的安全保障体系，导致网络安全厂商形成以合规思路设计产品和客户网络安全方案的惰性思维，也造成了过去行业多年的同质化竞争、低价竞标。习总书记在2018年4月的全国网络安全和信息化工作会议上提出，要“加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然”，因此网络安全要和信息化系统建设同步，真正让安全成为“内生”。安全企业也需要与集成商、研究院和设计院一起，基于动态综合防御体系进行规划，实现信息化和安全同步规划、同步建设和同步运营。咨询规划又可以分为三类：安全规划、合规咨询、专项咨询。其中安全规划又可以分为安全规划和行业咨询；在合规咨询中又包括等级保护和分级保护的咨询、RT001、内服外省、热点事件的合规咨询等；专项咨询又包括：业务应用的安全咨询、数据安全的咨询服务、工业安全、安全研究报告等。2 运营服务　人、数据、工具、流程，共同构成了安全运营的基本元素，以威胁发现为基础，以分析处置为核心，以发现隐患为关键，以推动提升为目标通常是现阶段企业的安全运营的主旨。不管是基于流量、日志、资产的关联分析，还是部署各类安全设备，安全运营最终目标是了解企业自身安全情况、发现安全威胁、敌我态势、规范安全事件处置情况，提升安全团队整体能力，逐步形成适合企业自身的安全运营体系，并通过成熟的运营体系驱动安全管理工作质量、效率的提高。运营服务是过去几年安全服务增长最快的一个类目，因为增长快且能更加了解客户的网络安全状况并增强客户粘性，得到各大安全厂商的重视。运营服务内容又分三大类：基础运维服务、安全监察服务、巡查服务。目前全国多地在智慧城市中会设立一些安全运营中心，其中的核心服务就是安全运营服务。企业信息安全建设初期，在网络层、系统层、应用层、数据层等部署了一系列安全设备和管控措施进行日常运维，并确保其稳定运行。安全运营的核心是安全运维框架，承载安全运维框架的是SIEM平台或SOC平台。传统SOC平台缺乏安全攻防对抗能力，因为以安全日志和时间采集为基础对事件被动进行分析和响应；缺乏大量数据处理能力，因为传统SOC以关系型数据库为底层数据架构，处理能力相当有限，在海量数据、异构数据、多维数据的情况下，采集、分析和处理、存储数据都遇到很大困难。同时传统SOC平台缺乏安全智能分析能力、缺乏有效协同能力，因此安全龙头企业都纷纷推出了新一代威胁感知系统，再结合级的安全分析服务，为政企客户提供优

质体验的安全运营服务。　3 专业技术服务 通常包括攻防渗透、评估加固、应急响应。以奇安信对运营商提供的专业安全服务解决方案为例，对运营商指定业务系统提供渗透测试、代码审计、新系统上线安全评估、移动APP加固等服务等安全服务，并提供应急响应服务。Web应用系统的渗透测试主要对操作系统及服务漏洞、应用系统漏洞、安全配置缺陷、功能逻辑缺陷等方面进行全面测试，APP应用系统还需要对APP客户端漏洞进行针对性测试。源代码审计服务的目的在于充分挖掘当前源代码中存在的安全缺陷以及规范性缺陷，从而让开发人员了解其开发的应用系统可能会面临的威胁，并指导开发人员正确修复程序缺陷，通过对系统开发框架、应用程序、客户端程序（包含APP应用程序、C/S客户端等）、接口及第三方组件和应用配置这五个方面进行深入的安全分析，从而发现系统源代码存在的安全缺陷，并采用安全测试等技术手段进行漏洞验证。同时新系统上线前进行渗透测试及源代码审计等安全服务，从黑盒测试和白盒评估两个层面发现系统可能存在的安全风险，最大限度的解决安全问题，减小了系统投产后的安全风险。而应急响应服务一般是机构、企业的网站、办公区终端、核心重要业务服务器或邮件服务器遭到了攻击，影响了系统运行和服务质量，因此需要安全供应商在发生攻击事件时提供应急人力保障、技术手段保障、技术支撑保障。重保活动的网络安全保障：近年来我国重要活动或者会议的组织方和网络安全监管机构都要求在活动或者会议期间开展网络安全重保工作，以确保重要活动或者会议的圆满顺利完成。重保对象一般是主办方的信息系统和举办场地有关的网络环境、互联网各类宣传通道；监管机构的内部信息系统和其他可能涉及的党政机关、金融、媒体、交通、能源、水利、教育等行业的重要信息系统。重保除了需要专业的技术团队，还需要工具和技术平台配合，包括互联网资产发现与扫描平台、高级威胁监测平台、攻防演练平台、网站安全监测平台、网站安全云防护平台和安全态势感知平台等。　4 安全演练 2016年开始国家监管机构每年组织开展针对不同行业、地域的网络实战攻防演练，且涉及的行业范围越来越广，尤其是关键信息基础设施的运营者会积极国内网络攻防实力较强的网络安全企业对其所负责的关键信息基础设施开展真实环境下的网络攻防演练。实战攻防演练以实战化、可视化、专业化为原则，对实际目标系统以不进行破坏攻击为底线，进行实战攻防对抗，攻击模式不限于单个系统，不限于内网渗透，不限于通过周边系统迂回，一般希望达到以下目的：a)拿到目标业务系统的控制权限；b）深入挖掘机构、企业信息系统可能存在的安全风险；c)全面检验机构、企业网络安全防御体系的有效性；d）检验机构、企业人员的应急响应能力和协作配合能力；e）促进机构、企业增强网络安全意识、认清所面临的网络安全风险、完善网络安全保障体系。通过对攻击者主要攻击思路和攻击手法的了解，机构、企业可以有针对性地在攻击实施的各阶段做好安全检测、分析、处置和防御等工作，发现存在的薄弱环节和漏洞，并在演练后的总结复盘过程中，根据详尽的安全整改建议，提高网络安全防御能力。现实场景中通过红、蓝、紫

三方的真实对抗，红方为企业、机构内部安全人员，负责内部防护；蓝方为机构、企业外部人员（白帽子），负责外部攻击；紫方为机构、企业外部教练（一般为安全厂商），负责提供安全演练导调、监控进程、全程指导、应急处置、活动总结等咨询工作。 5 数据分析 要做到主动安全和监测需要数据分析支撑，数据分析主要分两大类：威胁情报、安全数据分析，安全服务中数据分析不仅需要对监测到的安全数据进行报告和处置，进行进一步的安全数据分析、溯源和研判；还需要对安全数据进行整理形成通报结果，与客户的网络安全工作职能相对接，开展信息安全风险报告和信息通报等工作。以奇安信为例，利用云端威胁情报，为客户提供来自外部的攻击态势，对攻击者进行精准的多维属性分析，形成外部攻击者画像；分析客户资产的暴露面，发现未知资产；结合内部流量数据，为客户提供数据分析服务，进行外部攻击分析、主机失陷分析、内部安全分析，协助客户建设全天候、全方位的网络安全态势感知能力。态势感知安全服务帮助企业做好内网检测和防御，具备全方位的感知能力，感知是依托于大量数据的反馈，因此需要统一的日志收集和分析平台，平台要具备持续的威胁检测，通过各种检测规则和机器学习模型来对所有收集到的日志进行匹配检查以保证之前的已知威胁不会被忽略。现阶段基于威胁情报的IOC检测平台也不可或缺，用来对外部情报信息或者内部自产的情报信息进行实时匹配和报警以确保当前所有的已知威胁能被检出。还需要流程管理平台配合，其主要作用是用于流程化和规范化地记录和总结所有以往发生的入侵事件的调查过程和分析结果，以便于日后查询和关联分析，同时可以用于追踪考核。威胁情报是对企业产生潜在与非潜在危害的信息集合，帮助企业判断当前发展现状与趋势，并可得出所面对的机遇和威胁，再提供相应的决策服务。国内外都有专门提供威胁情报的公司，如微步在线、天际友盟、安天科技和默安科技。 6 考试与培训 又可以细分为：认证培训、联合培养等等。认证培训里面又可分为证书的认证培训，包括考试与培训工具。安全培训也有安全能力建设，包括攻防技术、产品认证、安全运营培训等。另外一个就是联合人才培养。我国目前网络安全运营人才需求较大，无论是企业还是政府对网络安全人才需求都呈现快速增长趋势。根据网易调查显示，2019年安全运营与服务类的岗位需求大幅增长，成为政企机构招聘最多的岗位类型，占比高达32.7%，首次超过研发测试岗位。 2019年上半年，网络安全人才需求规模指数为117.2，较2018年下半年环比增长104.9%，较2018年上半年同比增长173.2%。其中安全运营与服务类岗位是政企需求量最多的岗位，占32.7%，其次是研发与测试类岗位25.0%，销售类占11.7%。2018年-2019年度包括中央网信办、工业和信息化部、公安部等在内的监管部门发布一系列法规或规章中，很多措施明确要求设置网络安全专员。2019年上半年正式发布国家标准《信息安全技术网络安全等级保护基本要求GB/T22239-2019》也将网络安全机构设置和管理制度纳入国家统一标准里，机构建立和机制完善很可能持续带动安全人才需求的爆发式增长。同时很多大中型或大型企业，已经开始着手逐步建立自己

的专业安全团队，以应对企业面临的网络安全日常威胁与突发事件，因此对安全、安全顾问，及高级网络安全管理人员的需求也大幅增加。网络安全领域考试众多，根据调查，超半数的新晋网络安全人才听说过CISP、NISP，40%以上的网络安全人才听说过CISP-PTE以及CISSP。政企机构网络安全人才岗位需求分布　　中企顾问网发布的《2022-2028年中国网络公共安全市场深度分析与市场调查预测报告》共十章。首先介绍了中国网络公共安全行业市场发展环境、网络公共安全整体运行态势等，接着分析了中国网络公共安全行业市场运行的现状，然后介绍了网络公共安全市场竞争格局。随后，报告对网络公共安全做了重点企业经营状况分析，最后分析了中国网络公共安全行业发展趋势与投资预测。您若想对网络公共安全产业有个系统的了解或者想投资中国网络公共安全行业，本报告是您不可或缺的重要工具。
本研究报告数据主要采用国家统计数据，海关总署，问卷调查数据，商务部采集数据等数据库。其中宏观经济数据主要来自国家统计局，部分行业统计数据主要来自国家统计局及市场调研数据，企业数据主要来自于国统计局规模企业统计数据库及证券交易所等，价格数据主要来自于各类市场监测数据库。 报告目录：第.一章 网络公共安全行业产品定义及行业概述发展分析第.一节 网络公共安全行业产品定义一、网络公共安全行业产品定义及分类二、网络公共安全行业产品应用范围分析三、网络公共安全行业发展历程四、网络公共安全行业发展地位及影响分析第二节 网络公共安全行业产业链发展环境简析一、网络公共安全行业产业链模型理论二、网络公共安全行业产业链示意图及相关概述第三节 经济环境一、国民经济运行情况GDP （季度更新）二、消费价格指数CPI、PPI （按月度更新）三、全国居民收入情况（季度更新）四、恩格尔系数（年度更新）五、工业发展形势（月度更新）六、固定资产投资情况（季度更新）七、2020年我国宏观经济发展预测第四节网络公共安全行业税收及进出口关税第五节 社会环境一、 人口数量及老龄化分析二、网民规模情况三、90后消费群体特点分析第六节网络公共安全技术发展现状一、网络公共安全行业技术发展二、网络公共安全生产工艺一、网络公共安全技术发展趋势 第二章 2015-2019年网络公共安全行业国内外市场发展概述第.一节2015-2019年全球网络公共安全行业发展分析一、全球网络公共安全经济发展现状及预测二、全球网络公共安全行业技术发展现状三、全球网络公共安全行业发展概述第二节2015-2019年全球网络公共安全行业供需及规模分析一、全球网络公共安全行业市场供需情况二、全球网络公共安全行业市场规模及区域分布情况三、全球网络公共安全行业重点国家市场分析四、全球网络公共安全行业发展热点分析五、2022-2028年全球网络公共安全行业市场规模预测第三节2015-2019年中国及全球网络公共安全行业对比分析一、中国网络公共安全行业生命周期分析二、中国网络公共安全行业市场成熟度情况三、中国和国外网络公共安全行业对比SWTO第四节2015-2019年全球网络公共安全所属行业相关产品进出口情况 第三章 2015-2019年我国网络公共安全行业发展现状第.一节 中国网络公共安全行业发展概述一、中国

网络公共安全行业发展现状　　由于安全保密因素，目前仅有3家公司拥有全资质。国家对于从事网络公共安全领域的企业有资质要求，其中仅3家（烽火星空、锐安科技、太极股份）具有完整业务资质。由于资质要求较高，特别是全资质企业都是早期授予的，而且出于安全考虑未来政府继续增加授予新企业资质的可能性很低，该行业有较高的资质壁垒。　　烽火星空是该领域的行业龙头，是最早期进入该领域的企业之一，拥有最全的网络公共安全业务资质，早期烽火星空的解析技术以及全文检索分析技术为其技术优势，凭借快速客户响应，一流服务能力，迅速抢占全国60%以上的市场份额；如今公司已发展至2000余人，覆盖全国200多个城市。锐安科技也是最早期进入该领域的企业之一，拥有全网络公共安全资质。目前，公司员工数1000余人，业务覆盖全国200多个城市，市场份额为烽火星空的一半。太极股份通过收购网络安全相关团队进入该领域，业务种类较多，进入安全业务领域后该业务处于未盈利状态，覆盖客户点相对较少。网络公共安全行业市场格局二、中国网络公共安全发展面临问题三、2015-2019年中国网络公共安全行业市场规模四、中国网络公共安全行业需求客户结构第二节 我国网络公共安全行业发展状况一、2015-2019年中国网络公共安全行业产值情况二、2019年我国网络公共安全产值区域分布分析第三节 2015-2019年中国网络公共安全行业产量分析第四节 2019年网络公共安全行业需求分析一、2015-2019年我国网络公共安全行业需求分析二、2015-2019年我国网络公共安全市场价格走势分析 第四章 网络公共安全行业竞争态势分析第.一节 网络公共安全行业集中度分析一、网络公共安全市场集中度分析二、网络公共安全企业分布区域集中度分析三、网络公共安全区域消费集中度分析第二节网络公共安全行业主要企业竞争力分析一、重点企业资产总计对比分析二、重点企业从业人员对比分析三、重点企业全年营业收入对比分析四、重点企业利润总额对比分析五、重点企业综合竞争力对比分析第三节 网络公共安全行业竞争格局分析一、2019年网络公共安全行业竞争分析二、2019年中外网络公共安全产品竞争分析三、2019年我国网络公共安全市场竞争分析四、近年国内网络公共安全行业重点企业发展动向 第五章 2015-2019年中国网络公共安全所属行业运行及进出口分析第.一节 2015-2019年中国网络公共安全所属行业总体运行情况一、网络公共安全企业数量及分布二、网络公共安全行业从业人员统计第二节 2015-2019年中国网络公共安全所属行业运行数据一、行业资产情况分析二、行业销售情况分析三、行业利润情况分析第三节 2015-2019年中国网络公共安全所属行业成本费用结构分析第四节 2015-2019年中国网络公共安全所属行业经营成本情况第五节 2015-2019年中国网络公共安全所属行业管理费用情况第六节 中国网络公共安全所属行业或相关行业进出口分析1、2015-2019年所属行业进出口数量及金额2、行业进口分国家3、行业出口分国家 第六章 2015-2019年中国网络公共安全行业区域发展分析第.一节 中国网络公共安全行业区域发展现状分析第二节 2015-2019年华北地区一、华北地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测

第三节 2015-2019年东北地区一、东北地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测第四节 2015-2019年华东地区一、华东地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测第五节 2015-2019年华南地区一、华南地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测第六节 2015-2019年华中地区一、华中地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测第七节 2015-2019年西部地区一、西部地区经济发展现状分析二、市场规模情况分析三、市场需求情况分析四、行业发展前景预测第七章 网络公共安全重点企业发展分析第.一节 A公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析第二节 B公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析第三节 C公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析第四节 D公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析第五节E公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析第六节F公司一、企业经营情况分析二、企业产品及竞争优势分析三、市场营销网络分析四、公司战略规划分析 第八章 2015-2019年中国网络公共安全行业上下游主要行业发展现状分析第.一节 2015-2019年主要上游产业发展分析一、A行业发展分析1、行业市场规模情况2、产品价格分析3、产品生产情况二、B行业发展分析1、行业市场规模情况2、产品价格分析3、产品生产情况……第二节2015-2019年主要下游产业发展分析一、D行业发展分析1、行业现状分析2、行业发展前景二、E行业发展分析1、行业现状分析2、行业发展前景……第九章 2022-2028年中国网络公共安全行业发展预测分析第.一节2022-2028年中国网络公共安全行业产量预测第二节2022-2028年中国网络公共安全行业需求量预测第三节2022-2028年中国网络公共安全行业规模预测第四节 2022-2028年中国产业的前景及趋势一、中国网络公共安全市场发展前景乐观二、2020年中国网络公共安全市场消费趋势分析第五节2022-2028年中国网络公共安全行业发展趋势一、中国网络公共安全行业的发展前景二、2022-2028年中国网络公共安全产业规划分析三、我国网络公共安全行业的标准化发展趋势第六节2022-2028年中国网络公共安全行业“走出去”发展分析 第十章 网络公共安全行业投资前景研究及销售战略分析()第.一节 影响网络公共安全行业发展的主要因素一、影响网络公共安全行业运行的有利因素二、影响网络公共安全行业运行的稳定因素三、影响网络公共安全行业运行的不利因素四、我国网络公共安全行业发展面临的挑战五、我国网络公共安全行业发展面临的机遇第二节 行业投资形势分析一、2015-2019年中国行业投资规模二、行业投资壁垒三、行业SWOT分析四、行业五力模型分析第三节 2022-2028年网络公共安全行业投资效益分析第四节 2022-2028年网络公共安全行业

投资前景研究研究第五节 网络公共安全行业投资前景预警一、2022-2028年网络公共安全行业市场风险预测二、2022-2028年网络公共安全行业政策风险预测三、2022-2028年网络公共安全行业经营风险预测四、2022-2028年网络公共安全行业技术风险预测五、2022-2028年网络公共安全行业竞争风险预测六、2022-2028年网络公共安全行业其他风险预测第六节 市场策略分析一、网络公共安全价格策略分析二、网络公共安全渠道策略分析第七节 销售策略分析一、媒介选择策略分析二、产品定位策略分析三、企业宣传策略分析第八节 提高网络公共安全企业竞争力的策略一、提高中国网络公共安全企业核心竞争力的对策二、网络公共安全企业提升竞争力的主要方向三、影响网络公共安全企业核心竞争力的因素及提升途径四、提高网络公共安全企业竞争力的策略第九节 对我国网络公共安全品牌的战略思考一、网络公共安全实施品牌战略的意义二、网络公共安全企业品牌的现状分析三、我国网络公共安全企业的品牌战略四、网络公共安全品牌战略管理的策略第十节 市场的重点客户战略实施一、实施重点客户战略的必要性二、合理确立重点客户三、重点客户战略管理四、重点客户管理功能() 图表目录：图表：网络公共安全行业历程图表：网络公共安全行业生命周期图表：网络公共安全行业产业链分析图表：2015-2019年网络公共安全行业产能分析图表：2015-2019年网络公共安全行业市场规模分析图表：2015-2019年网络公共安全行业产量分析图表：2015-2019年网络公共安全行业需求量分析图表：2019年网络公共安全行业需求领域分布格局图表：2022-2028年网络公共安全行业市场规模预测图表：中国网络公共安全行业盈利能力分析图表：中国网络公共安全行业运营能力分析图表：中国网络公共安全行业偿债能力分析图表：中国网络公共安全行业发展能力分析图表：中国网络公共安全行业经营效益分析图表：2022-2028年网络公共安全行业市场规模预测图表：2022-2028年网络公共安全行业产量预测图表：2022-2028年网络公共安全行业需求量预测更多图表请见正文……

详细请访问：http://www.cction.com/report/202112/259838.html